MASTER'S THESIS

Privacy-Sensitive Design for privacycompliant applications

How developers can implement privacy values and Privacy by Design in their process.

van den Berg, R.

Award date:
2020

Privacy-Sensitive Design for privacy-compliant applications

How developers can implement privacy values and Privacy by Design in their process.

Degree programme:	Open University of the Netherlands Faculty of Management, Science & Technology Business Process Management & IT master's programme
Course:	IM9806 Business Process Management and IT Graduation Assignment
Student:	R. van den Berg
Identification number:	
Date:	2nd of May 2020
Thesis supervisor:	Dr. R. Bosua
Co-reader:	Dr. L.H.H. Bollen
Version number:	2.7
Status:	Final

ABSTRACT

The introduction of the GDPR sparked a lot of discussion on privacy and already resulted in penalties for data processors for not complying with the regulation. One of the requirements enforced by the GDPR is building applications using P*rivacy by Design*. To determine how more 'privacy-compliant' applications can be created, an exploratory qualitative research design has been conducted using a case study approach in this study. Findings are based on interviews performed in two educational organisations. The findings reveal that both employees (as users) and software developers value privacy, although they do not always act on it. Both users and developers see the need to adapt to *Privacy by Design* principles and the use of the *Value Sensitive Design* method during software development, as beneficial for applications. Users also indicate that they would like to give more input relating to the design of privacy-embedding software applications. The research concludes that using a set of privacy principles and a method when developing these applications, could add to more 'privacy-compliant' applications that can be more GDPR compliant, which both allow for more future research. Although the study has some limitations with respect to external validity, the study's findings can be applied to increase software development teams' awareness and incorporation of privacy as a value in new applications. The research contributes to the body of knowledge in information science on how software developers can create more GDPR compliant applications.

KEY TERMS

Privacy by Design (PbD), Value Sensitive Design (VSD), Application development, GDPR, Privacy, Value of Privacy.

ACKNOWLEDGEMENTS

I would like to acknowledge everyone who played a role in the realization of this thesis. Without this help and attention I would not have been able to achieve this academic accomplishment. A special notice to my wife Annemieke, with whose patience, love and comforting words I have been able to reach this milestone after years of studying, alongside raising our three beautiful children. This would not have been possible without you. I would also like to thank my thesis supervisor, Dr. Rachelle Bosua, who provided attention, time and guidance to get this research to the academic level it is. I appreciate the effort, the discussions we have had, extensive feedback, insightful input and directions I have received. Also, I want to thank the interviewees and participating case organisations, I am thankful for their time and co-operation. Furthermore, I want to thank Dr. Laury Bollen for co-reading and giving constructive feedback. Lastly, I want to thank the Open Universiteit for the path that led me to the finish, this thesis.

SUMMARY

The research focuses on the embedding of privacy within software application development. The results are projected on the two interviewed target groups: employees as users and internal developers of the same organization who develop software for its employees. Two educational institutions, both universities, each with its own software development capabilities in house were selected to participate in this study. Interviews focused first on employees' thoughts on privacy, their views on the value of privacy, the creation of applications using Privacy by Design (PbD) principles and an approach to do so: The Value Sensitive Design (VSD) method. Developers were asked similar questions, but also how they thought users would react on PbD principles and the VSD method.

The results indicate that users value their privacy, but they do not always act on it. They often trade their privacy for other functionalities or social services. This was also the same for developers. In general, users had little interest or knowledge of the GDPR regulation in this context, although they heard about the GDPR and knew it aimed at protecting individuals' privacy. When presented with the seven PbD principles and the VSD method, users reacted positively and indicated this would contribute to more privacy-compliant applications. Developers also confirmed this fact. Furthermore, developers seemed to appreciate the GDPR more than users, seeing it as a positive contribution to application development. Although none of the developers were aware of the seven PbD principles nor the VSD method, they were positive about the contribution both could bring to application development. Developers did not expect that users would be enthusiastic when presented with both PbD and the VSD method.

In conclusion, this study confirms that the use of the principles from the VSD method, could help embedding Privacy by Design and end-user privacy values into software applications. By doing so, applications can become more 'privacy-compliant' and therefore ultimately contribute to software applications being more GDPR compliant. Although this research has limitations mainly due to the generalizability, the findings provides more guidance how software development teams can improve privacy-related aspects of their applications. The research gives some advice for future research, for example: does adaptation to PbD lead to applications which are more legally compliant with the GDPR? Future research could also focus on the practical aspects of embedding PbD principles in software development processes.

Contents

KEY DEFINITIONS

GDPR Compliant	Having implemented technical and operational safeguards to protect personal data to meet GDPR regulation (EU, 2016) i.e. in this context, privacy embedded within software development and design.
Individual privacy	A preservation of autonomy, a release from role-playing, a time for self-evaluation and for protected communication (Westin, 1967).
Privacy by Design	The embedding of privacy during the development process of an application (Cavoukian, 2009).
Privacy compliant	In agreement with a set of rules to assure the privacy of the user(s) (Oxford, 2020). In this context the set of rules being GDPR, principles of VSD and PbD.
Software development process	A software development process contains a series of tasks that provide a structure for developing and maintaining applications (ISO/IEC/IEEE, 2017).
Value of privacy, privacy values	The illumination of (individual) privacy depending on the purposes of the practices involved (Solove, 2002). In this context the practice of using applications.
Value Sensitive Design	Value Sensitive Design is a theoretically grounded three staged approach to design technology that accounts for human values (in this context 'privacy' as a value in a principled and comprehensive manner throughout the software development process (Friedman, Kahn, & Borning, 2002).

1. INTRODUCTION

At the time of writing this thesis, the General Data Protective Regulation (GDPR) has passed its 3-year anniversary. The first stages of this regulation were found in the beginning of 2012 where the European Commission proposed an extensive reform of the existing privacy legislation. The trajectory resulted in approving the GDPR 4 years later in 2016. Two years later the legislation came into effect in on 25 May 2018. Despite the long lead, companies still have problems with GDPR compliance, where 80% of the companies admit that *"it was equally or more difficult to implement than other data privacy and security requirements"* (Ponemon, 2019). GDPR compliance particularly for software applications, is important for European companies, consumers and governments, also non-European companies serving customers in Europe. The latter may already be the case if prices are displayed on a website in Euros.

For companies to become compliant with GDPR legislation they need to adapt their application development processes. Hence, this study focusses on how businesses can adapt their software development processes to create more GDPR compliant applications. Where privacy can be seen as the cornerstone of GDPR legislation, embedding privacy as a value in the design of software can be seen as a manifestation of Value Sensitive Design[1] in the context of privacy legislation. Furthermore, this study aims to extend existing knowledge on the development of privacy-compliant software applications.

1.1. BACKGROUND

The first research published regarding individual privacy has been broadly discussed since the late 1800's and marked the beginning of a thoroughly researched discipline (Warren & Brandeis, 1890). In this article the authors conceptualize the "right to be left alone". This article is generally observed as a landmark in privacy regulation. In 1948 the Universal Declaration of Human Rights already stated in article 12: "*Anyone has the right to be protected against interference with his or her privacy"* (UN, 1948). Europe started in the early 1980's with privacy regulation with the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (known as convention 108). Followed up by the predecessor of the GDPR: The Data Protection Directive (1995, known as directive 95/46/EC). In April 2016 came the GDPR in effect (EU, 2016), which is being enforced since May 2018. The introduction of the GDPR was accompanied with much attention from consumers, lawmakers and companies. This was not only because of the far-reaching rights for consumers, but also because of the measures that could be imposed on companies in the event of non-compliance with the GDPR (Espiner, 2018). An eye-catching sanction is the fine that can amount to a maximum of 4% of an organisation's annual turnover. This mean that companies can receive fines of up to billions. An example is British Airways who recently faced a +€200 million fine by the British ICO for violation of GDPR law (Cellan-Jones, 2019).

The creation of privacy law and regulation is driven by the desire of the people to ensure their privacy rights. This study therefore investigates whether the underlying values and Privacy by Design (PbD) principles of privacy legislation can be used within or as part of the concept of Value Sensitive Design (VSD), i.e. the design of software systems and applications that take into account human values by embedding privacy as a value into the whole design process. Incorporating VSD principles in the software development process will result in creating applications that meet regulatory privacy requirements without limiting the possibilities of meeting business goals.

[1] Or: Design for Values, for this study the term '*Value Sensitive Design*' will be used.

1.2. CONTEXT

The GDPR introduces a firmer set of rights for individuals in relation to their privacy aspects. This brings a dilemma to companies. On the one hand they want to use individuals' data to meet their business goals. On the other hand, they have to pursue maximal GDPR compliance. Companies use data for creating business value by using it for marketing, finance, supply chain management, etc. (Provost & Fawcett, 2013). In this way, (the use of) data gets a more prominent place within the creation of propositions for costumers.

In 2019, almost all of the larger tech companies (Google, Amazon and Apple) were exposed for violating customers' privacy (Leijten, 2019). Information disclosure of these companies concerned their voice assistants, where speech commands, even unintentionally, recorded conversations that were being recorded and analysed by tech companies. These companies claim they needed the data to improve their products and services, but consumers were not informed nor consented to the collection and use of their data for product and process improvement.

The GDPR starts with 173 recitals, and following these, continues with 99 articles. The first recital emphasizes the importance the EU attaches to the GDPR: *"[…]The protection of natural persons in relation to the processing of personal data is a fundamental right"* (EU, 2016). The GDPR refers to Privacy by Design when developing applications, to express this more strongly, the 7 principles that Ann Cavoukian (2009) has set out are used in this study.

A fairly new research field within Information Sciences (IS) is Value Sensitive Design (VSD). In the mid 90's an effort has been made to create a framework to incorporate user values within the design of software and systems (Friedman & Nissenbaum, 1996). The main goal was to prevent bias to influence the creation of new systems and applications. This research and ideas accumulated into the creation the Value Sensitive Design framework (Friedman, 1997). The concept was first coined one year following Friedman's publication regarding bias in computer systems (1996).

For this study, the focus is *whether the principles of Value Sensitive Design (VSD) and Privacy by Design (PbD) can help companies create privacy-compliant applications which are more GDPR proof*. Therefore, we consider the importance of Privacy as a Value.

1.3. RESEARCH OBJECTIVE AND QUESTIONS

The above paragraphs give the context about the urgency for companies to comply with GDPR regulation. The foundation of the GDPR lies in shared values of EU citizens, which motivates politicians and legislators to create corresponding legislation focused on protecting a person's personal data or personal information. The values which rooted in the legislation should be used to create applications that takes these values into consideration. Due to the lack of research on the combination of the underlying value of privacy within VSD and how companies can use the principles VSD to improve data subjects' rights, the problem that will be addressed through the following main research question is:

How can Value Sensitive Design and 'Privacy by Design' embed Privacy Values into software development to develop applications that are more GDPR compliant?

This main research question will be further divided into sub research questions which will be formulated following the literature review in chapter 2.

1.4. RESEARCH APPROACH

To give a satisfactory answer to the main research question and forthcoming sub research questions, a qualitive research approach using a case study as a research strategy (Saunders, 2016).

This approach will be grounded by conducting interviews within two large educational institutions following a qualitative approach (Saunders, 2016). After the literature review, a conceptual model is developed which will be evaluated within two case organisations as part of the empirical part of this thesis.

1.5. Overview

This thesis will continue in the next chapter with a literature review on the key concepts of VSD, Privacy (by Design), and the GDPR in the context of IS. This chapter will also highlight the process that has been followed to gather and analyse literature. After presenting the findings a conceptual model and sub research questions will be derived from the analysed literature. Chapter 3 will focus extensively on the followed research methods, how data has been collected, where, from whom and how it has been analysed. Chapter 3 will also discuss how construct validity has been grounded within the research. Chapter 4 will present the empirical collected data. The thesis will conclude with a discussion and answer on the research questions in chapter 5, describe relevant limitations of (the execution of) the study and provide implications of this research for academia or practice.

2. THEORETICAL FRAMEWORK

In the previous chapter, an overview was presented regarding the main research question alongside the aim and broader context of this research. Continuing in this chapter, is a set of relevant literature relating to the concepts and main research questions derived from an analysis of the collected literature. Performing a solid literature review is essential prior to any academical project (Webster, 2002), it gives context and perspective on the subject of study and concepts that are relevant in a study. At first the approach will outline how the literature study has been performed. After the approach has been clarified, the results of the literature compilation will be discussed. Finally, in the last paragraph of this chapter, a synthesis will follow of themes from the literature leading to a model and sub research questions, which will be subjected to validation during the remainder of this study.

2.1. RESEARCH APPROACH FOR THE LITERATURE ANALYSIS

First, an outline is presented on how the gathering of relevant literature has structurally been executed. For this, the study resorted to the "Grounded theory method" (Wolfswinkel, Furtmueller, & Wilderom, 2013). Within a few steps, an iterative and structured cadence is being outlined by Wolfswinkel et al. (2013) for gathering literature. This resulted in the following approach for his study:

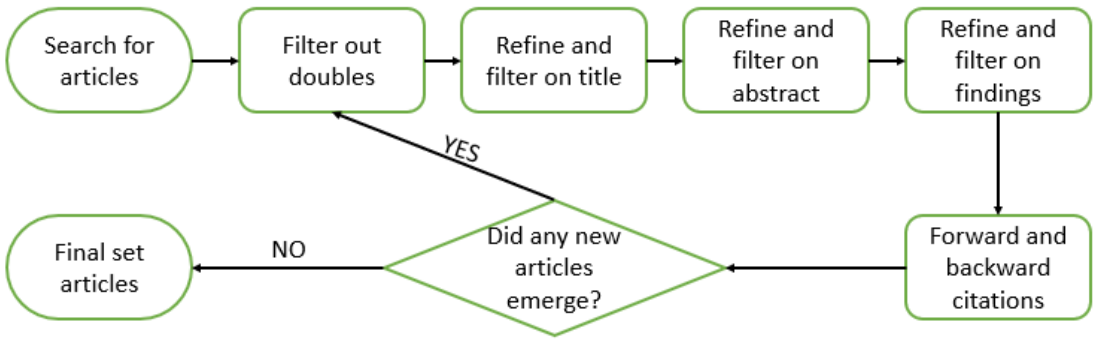


Figure 1 Process for gathering literature, based on Wolfswinkel et al (2013)

For the structured presentation of the findings from the literature, the *concept matrix approach* from Webster and Watson (2002) was adapted, which resulted in a literature table to reflect the result of the above process.

Search method

Some criteria are applicable during the literature search. In principle, due to the newness of the topic, with the initial search, only articles from 2011 and later years were selected. Furthermore, for articles published in journals, a crosscheck was performed against the ABDC Journal quality list (ABDC, 2019). Only journals with an A*, A or B rating were used. If the journal is not enlisted in this overview list, a first impression was made by reviewing the content and if applicable the Google Scholar H5-score (Google, 2019).

The search for literature was performed by/in Google Scholar. If the found article, judged as relevant, was being blocked by a "paywall" the OU University library was consulted for direct access to the article.

For this study, the focus was on GDPR privacy regulation within the context of Value Sensitive Design, therefore the initial used search query used the following keywords: *"value sensitive*

design" AND "informed consent" AND GDPR. The second search was more focussed on the tension between privacy and the desire of data subjects regarding what they were willing to disclose, therefore the second search query was: *"value sensitive design" AND "informed consent" AND "Privacy Paradox".* The AND operator was used to ensure all items were included and the " " operators were used to ensure that the concept of VSD and informed consent were found as a whole. Otherwise Google was used to look for parts of the search terms within the given result.

Search Results, Selection and Analysis
The extensive search resulted in 332 (the first query: 296, and the second query: 36) articles from a variety of sources. The first sorting was by the criteria mentioned in the previous paragraph (Search method). After the initial sorting, the next selection was performed based on the paper's title and if this matched the subjects, concepts and context. In the third action a further drill down was performed on the source by analysing the abstract of each paper. If the abstract proved to be valuable for the study the source was included as a reference for further literature review. Finally, 15 articles have been selected, and were divided into one or more main themes, after a coding process (Wolfswinkel et al., 2013), as indicated in this table with the major themes that were covered in each paper:

MAJOR THEMES	ARTICLE
1. INDIVIDUAL PRIVACY	(Santanen, 2019; Warnier, Dechesne, & Brazier, 2015)
2. PRIVACY AS A VALUE	(Bashir, Hayes, Lambert, & Kesan, 2015; Brown, 2001; Kokolakis, 2017; Santanen, 2019; Solove, 2006; Warnier et al., 2015)
3. REGULATION ON PRIVACY DESIGN	(Cavoukian, 2009; Warnier et al., 2015)
4. VALUE SENSITIVE DESIGN	(Burmeister & Kreps, 2018; Cummings, 2006; Friedman, 1997; Friedman et al., 2002; Friedman, Kahn, & Borning, 2008; Ligtvoet et al., 2015; Warnier et al., 2015)
5. IMPLEMENTATION OF VSD	(Friedman et al., 2002; Friedman et al., 2008; Koops & Leenes, 2014; Ligtvoet et al., 2015; Spiekermann & Cranor, 2008; Warnier et al., 2015)

Table 1: Major themes that emerged from the literature analysis

The above list of relevant references encompasses empirical studies in relation to the concepts of GDPR, Privacy, Value Sensitive Design and informed consent. In the next paragraph a literature insight will be created of the found references in relation to the research question. Next to the collected literature the GDPR (EU, 2016) is obviously one of the sources that will be taken into account within the literature review.

2.2. RESULT OF THE LITERATURE REVIEW

The following paragraphs will provide an overview of the relevant themes derived from the literature in the areas of privacy, GDPR and Value Sensitive Design. The section classification corresponds to the themes found in accordance with the table in the previous chapter.

2.2.1 Individual privacy

Until the beginning of the 19th century privacy was not really a big issue. The first photographs taken of people required a long period of sitting or standing still (without smiling). Consent was therefore implied by taking the time and effort to have your picture taken. After photography took a flight and the printed press started to develop, Warren and Brandeis (1890) published an article about the right of being left alone. This article is being considered as the first appeal to protect an

individual's privacy. To illustrate privacy it can be framed from three points of view: first as the right to be left alone, second as personal control of the information about oneself and third the freedom of surveillance in the private space (Warnier et al., 2015). But why is privacy important? Looking from a philosophical standpoint one could argue first that privacy is crucial for the preservation of human dignity and secondly it is vital for maintaining personal relationships (Santanen, 2019).

2.2.2 The value of privacy

Digitization in the form of the rise of big data, automated processing and the gathering of data creates one of the greatest contemporary threats to individual's privacy. Never has it been easier to collect, process and spread collected data about individuals. It's noteworthy that these threats are overlooked or under-appreciated by many people (Bashir et al., 2015; Santanen, 2019; Warnier et al., 2015). Research indicates that there is a difference between what people feel and say regarding these threats and how they act if their privacy is under pressure. This contradiction between privacy attitude and privacy behaviour has been extensively researched as being the "privacy paradox" (Brown, 2001). Bashir et al.'s (2015) found that 92% of their study respondents agreed on the statement "Personal privacy is important to me" (n=756). Although acknowledging this statement, 81% of the respondents (n=727) stated that they submitted personal information online but wished they did not.

A single study (Kokolakis, 2017) has indicated that existing research on the privacy paradox phenomena is in fact contradictory due to the fact that studies have been performed within a different context. Moreover, privacy considerations differ from person to person (Kokolakis, 2017). To further complicate research on the privacy paradox men should consider the kind of threats an individual faces, within a given context. These threats have been elaborated structurally in an article by the model of Solove (2006), as shown in Figure 2 Solove's model. These threats serve to undermine one's freedom and individuality, also negatively impact a person's dignity (Santanen, 2019).

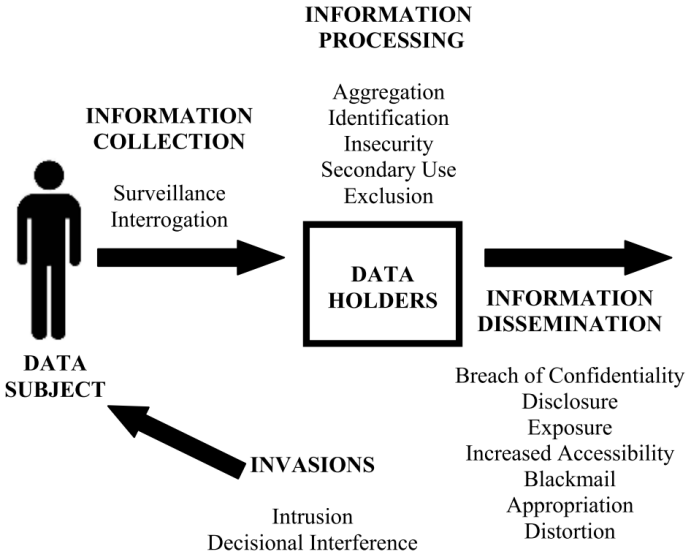


Figure 2 Solove's model (2006)

Due to the extensive description of threats by Solove (2006), the context of privacy and perception of privacy of an individual, it can be understood that it is complicated to conduct unambiguous research into this subject. Policy makers create legislation on privacy concerns as raised by the people, despite the inconsistency in the field of research on the privacy paradox (Kokolakis, 2017).

2.2.3 GDPR on privacy by design

Currently the most meaningful and advanced regulation (designed for EU citizens) on privacy is the GDPR (EU, 2016). The GDPR encompasses 99 articles and 173 recitals that provide explanations and context regarding the articles. These recitals give an indication of the idea behind these articles and express the importance that the EU attaches to privacy and its associated regulations. The second recital clearly shows the EU's goal with legislation on privacy (EU, 2016) as follows:

> *"The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."*

For application development, the GDPR also provides some starting points for companies to comply with these regulations. In article 25 of the GDPR, data controllers are subjected to use Data Protection by Design and by Default to meet the requirements as stated within the GDPR. Paragraph 2 of this article requires controllers to implement measurements for ensuring privacy by default and by design. Although article 25 paragraph 1 gives some examples, there is no exhausting explanation.

Privacy regulation is often formulated in a complex legal language and hard to interpret by engineers and designers (Warnier et al., 2015). To give more context to privacy by design, an engineer or developer can turn to the 7 foundational Privacy by Design principles as stated by Ann Cavoukian (2009). Her 7 principles encompass the following:

- Privacy by Design is proactive and preventive and is not to be done afterwards;
- Privacy should be the default, the practices she mentions are almost identical to the practices as stated in article 5 of the GDPR (EU, 2016);
- Privacy should be embedded in the design of new technologies, as secured in article 25 of the GDPR (EU, 2016);
- Functionality should not be restricted regarding to privacy design choices, an example within the GDPR is the notion regarding consent shouldn't be conditional (article 7, paragraph 4)(EU, 2016);
- Privacy protection and accountability should be present during the total life cycle of data;
- To establish trust visibility and transparency should be given regarding components and the process, this also is mentioned in the GDPR within article 5 paragraph 1a (EU, 2016);
- Finally, companies should respect their user's privacy by following the principles of Consent, Accuracy, Access and Compliance.

Practically a designer can achieve Privacy by Design by never processing any personal data or personal information. A second option is by applying strict privacy regulations when processing personal data. The last option is to only use anonymized personal data (Warnier et al., 2015).

2.2.4 Value Sensitive Design

Cavoukian's 7 principles give further insight into *the what*, but *not the 'how'* of incorporating privacy in systems and application. To successfully embed these principles in an application design process they have to be interpreted in the specific context of the application (Warnier et al., 2015). A unique method in the Information Systems domain to do so, is Value Sensitive Design (VSD) which is described as follows: This method considers human values in a theoretically grounded approach within the design process of (new) technology (Friedman et al., 2002). The method has

sprung from the idea that engineers develop their applications often from their own perspectives of values and primarily focus within the development process on functionality (Ligtvoet et al., 2015). Within the curriculum for application developers or software engineers, there has been little to no room to accommodate the ethical aspects associated with the design of software applications (Cummings, 2006). VSD is described as a method built on three separate stages that can be aligned with application development processes (Cummings, 2006) as outlined below:

Stage 1: covers conceptual investigation. In this stage a first analysis is performed on what values and (in)direct stakeholders are affected through the design process relating to a new system (Friedman et al., 2008). Although the involvement of all stakeholders is seen as a strong point of VSD, it must be borne in mind that not all stakeholders have appropriate ethical aspects. For example, one should assume that stakeholder values may be focused on protecting one's own dominant position (Burmeister & Kreps, 2018).

Stage 2: considers the empirical investigation to investigate the human context and if the application design works, when considering the context. This stage focusses on perceptible human behaviour (Friedman et al., 2002).

Stage 3: the last stage considers technical investigation where the technology at hand is being investigated in relation to human values (at stake) (Friedman et al., 2002; Friedman et al., 2008).

In a study regarding the *Dutch smart-meter case,* the researchers found 23 values which can be used within the VSD design process (Ligtvoet et al., 2015). Within the same context, van de Kaa et al (2019) continued an analysis of these values and found that privacy is being considered the most important value by the individuals affected within the case. Another interesting finding is that neglect of values within the design process can actually delay the implementation of a new technology (Ligtvoet et al., 2015).

2.2.5 Implementation of VSD

The implementation of 'values' within the application/software development process can help engineers and designers to develop better applications (Ligtvoet et al., 2015) by embedding the individual or user's value of privacy using VSD as a method into the application design process. The VSD method consists of the abovementioned three stages, focussing on individual's values: Conceptual Investigations, Empirical Investigations and Technical Investigations (Friedman et al., 2008). First of all, one should consider that implementation of human values does not, as with traditional design principles, require perfection but aims for commitment of the design team on ethical values (Friedman et al., 2002). One should also consider that there is no "golden bullet" approach on creating a privacy preserving system (Warnier et al., 2015). Roughly two approaches can be identified to implement the value of privacy using the VSD method: Privacy by Policy or Privacy by Architecture (Spiekermann & Cranor, 2008). Although the last one can possibly offer a higher level of privacy for users, it is nearly impossible to achieve GDPR compliance solely on techno-regulation by hard coding (Koops & Leenes, 2014). The privacy by policy approach seems better suited to adapt and has less interference with business models that need personal data to generate profit (Friedman et al., 2008; Spiekermann & Cranor, 2008).

An important note is that a key success factor for implementing VSD is to foster the right mindset and commitment of the design team (Cummings, 2006; Friedman et al., 2002; Koops & Leenes, 2014). One way to achieve this mindset is to create multi-disciplinary teams by adding a value subject-matter expert to the team (Cummings, 2006).

Some practical advice has been offered on how to put the VSD method into practice by Friedman et al (Friedman et al., 2008):

- Start with identifying the value(s) at stake or analyse the technology within the context in which this technology is being used. Issues relating to values will soon emerge;
- Systematically identify all the (in)direct stakeholders;
- Identify the pros and cons of all stakeholders, keeping in mind that they might have (un)ethical hidden agenda's (Burmeister & Kreps, 2018). Furthermore, be aware of the fact that like privacy, values are also perceived in a specific context (Friedman, Hendry, & Borning, 2017);
- Correlate identified pros and cons on applicable values;
- Use relevant literature to conduct research on identified values; and
- Identify conflicts between values.

Spiekerman and Cranor (2008) also offer practical advice and considerations for developers to achieve PbD as follows:

- Minimalize transfers and identify which transfers occur in a transparent way;
- Ensure that stored data is protected;
- Facilitate control over data for the data subjects;
- Understand how data breaches occur;
- Understand what user's expectations are regarding privacy-compliance of the system;
- Consider regulations regarding privacy and the current threat model;
- Design user friendly interfaces and notices regarding to privacy;
- Give users safe insight and access to their information;
- Understand relations with customers.

2.3. Research Questions and Conceptual model

In the literature there is a large body of research that can be found relating to Privacy, Privacy by Design and Value Sensitive Design. No literature has been found where research has focused on software becoming *GDPR compliant* by embedding the PbD and VSD principles in the software design process. The gap that has been identified is whether VSD can help implement Privacy by Design principles and the human value of privacy in the software design process. Hence, can software development teams create privacy-compliant applications which comply to the GDPR regulation? This leads to the main research question (MQ) that this thesis has to answer:

MQ: *How can Value Sensitive Design and 'Privacy by Design' embed Privacy Values into software development to develop applications that are more GDPR compliant?*

From the literature, three key themes arose that are related to the main research question. First the perception of privacy by users and how they are incorporated into the design process. This looks similar to the described privacy paradox (Brown, 2001) where users are said to value privacy the most (van de Kaa et al., 2019) but not always handle privacy in the way that they say they do (Bashir et al., 2015). To further delve into this contrast, it is important to find out how individuals value their privacy in relation to application usage and development process. Furthermore it is important to determine users' knowledge regarding GDPR regulation and possible threats based on Solove's model (Solove, 2006). Therefore, the first sub question (SQ) this research aims to answer is:

SQ1: *What are users views on the value of individual privacy in context of the software development process?*

The second key theme relates to the seven Privacy by Design principles as proposed by Ann Cavoukian (2009). Since there is no research how these principles can be incorporated in the software development (SD) process, the question is how can these principles be used in combination with the VSD process so that they are ultimately embedded within an application? Do

developers know about these principles and by applying them, can they help by relating these to GDPR compliance? Therefore, the second sub research question will be:

SQ2: *How can applications become more GDPR compliant from using principles of Privacy by Design in the software development process?*

The third key theme that arose indicating a gap in the research was the creation of applications using the VSD method (Friedman, 1997). To answer the main question, it is important to identify how the value of privacy can be embedded in the design and development process of an application. Therefore, it is important to find out how developers perceive the value of privacy i.e. whether they are familiar with the basics of privacy by design (Cavoukian, 2009) and whether they involve their users or even know what they want. From this a conclusion should be drawn on the usability of an approach like VSD in the development process to ensure the value of privacy.

SQ3: *How can applications become more GDPR compliant from using principles of Value Sensitive Design?*

Using these (sub) research questions and identified theory from Chapter 2.2 a conceptual model that can be derived from the literature for this study, shown in Figure 3 Conceptual Model.

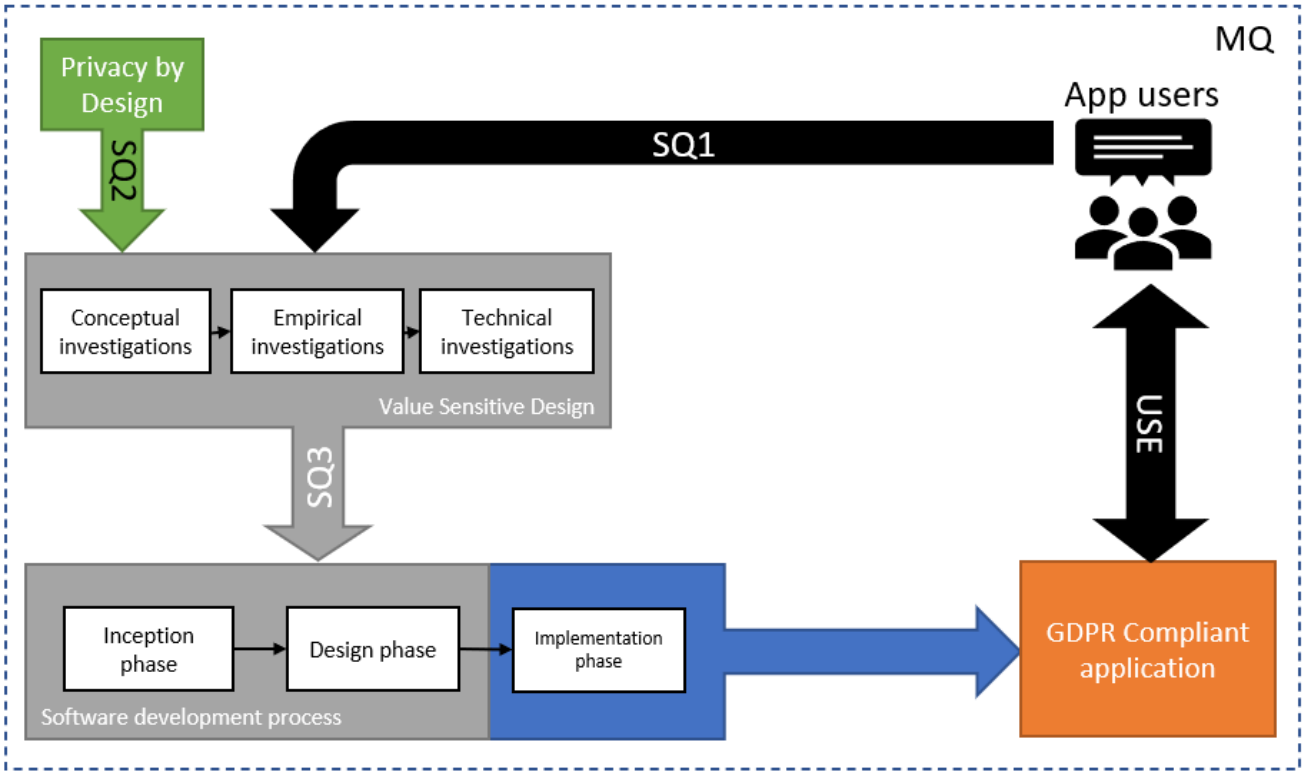


Figure 3 Conceptual Model

3. METHODOLOGY

Chapter 2 gives an overview of privacy, what the GDPR expects regarding Privacy by Design (PbD) and how VSD can be used to implement privacy policies relating to PbD. To evaluate these findings empirical research will be conducted.

This chapter will start with an overview of the different review approaches and continues with a detailed description of the blueprint that will be used to conduct this research. Paragraph 3.2 will elaborate on what method has been chosen and why. Paragraph 3.3 will paint a picture regarding the chosen case organisation. The final paragraph 3.4, will give insight on the arguments how this research conforms to validity, reliability and ethical aspects.

3.1. DIFFERENT TYPES OF RESEARCH APPROACHES

Within empirical research one has to distinguish between three types of research: Qualitative research, Quantitative research (the distinction between these two has been founded in the 80's by Lofland and Lofland (1984)), the third type is considered as a combination of both: the so-called mixed methods approach (Saunders, 2016).

The distinction between qualitative and quantitative is often made based on the data used within the research. Quantitative research often uses numbers to find a meaning, qualitative research often uses words. Other differences are to be found in the results: where quantitative research results often in numerical and standardised data, qualitative research results in rich data which needs to be classified by the researcher(s). A final distinction is the conceptualization: where quantitative research uses statistical calculations and diagrams, qualitative research uses conceptualisation for the analysis (Saunders, 2016).

Quantitative research mostly uses a deductive approach to test theories with gathered data, but it is also possible to use an inductive approach to generate a theory. *Qualitative research* is mostly used with an inductive approach, often associated with Eisenhardt (1989). However, using the research approach by Yin, it is possible to use qualitative methods to test a theory, therefore a deductive approach can be used (Yin, 2014). Finally, an iterative approach combining both can be used, named an abductive approach. The mixed methods research can use a combination of deductive, inductive and abductive approaches (Saunders, 2016).

To conclude: there are three strategies that can be used to perform the research: using experiments, surveys or case-studies. The approaches regarding these strategies differ on how data is collected, the way data is being analysed, the number of research objects, the selection of these research objects, the period of research and if the results can be checked (Braster, 2000).

For this thesis, a qualitative, interpretive approach is chosen. Since prior research on the topic is limited, the research would explore how and if principles of PbD and VSD can be embedded within the software development process to develop privacy-compliant applications.

3.2. RESEARCH DESIGN

The selection of an exploratory qualitative research approach is mainly based on the fact that no prior research has been found regarding the use of VSD to achieve GDPR compliancy. Furthermore the conceptualisation of privacy as a value and how this value is perceived, differs from person to person (Kokolakis, 2017). The use of interviews is an obvious method to drill down to the subject and the rich perceptions one has with respect to privacy values. To perform this research, a case-study method (within two educational organisations) was conducted. The selection of the case organisations was structured and conducted in a pragmatic and substantive way (Braster, 2000). This was mainly due to the researcher working already at one case organisation and having access to a second organisation. The following selection criteria for the case organisations were:

- The organisation should be engaged in the development of software;
- The organisation should be subject to GDPR compliance;
- There are at least 8 software developers working in the organization; and
- There must be access to the users for which the software is being developed.

The use of the case study method will deliver insights resulting from intensive and in-depth research of a phenomena within its natural context (Eisenhardt, 1989). Most frequently-mentioned disadvantages of a case-study is the fact that generalizability of the study's research results is difficult (Saunders, 2016).

The research should result in a discussion regarding the use of VSD and PbD to create privacy-compliant applications. Therefore, the composed sub research questions should be answered. To find the answer on the main question the empirical phase of the research is divided in two stages: The first stage is the collection of data and the second stage considers the analysis of the collected data as explained later in the next section.

To confirm reliability of this study, two similar organisations were used in a same context. This would add to generalizability and to look if there were differences to be found between the two organisations.

3.3. Participating Case organisations - description

The research took place using two large educational institutions (universities) as case organizations. Both are located in the Netherlands with over 10.000 students and more than 5.000 employees. The institutions are focused on (empirical) research and education.

The first institution has a central IT unit/department within the Management facility of the company. The IT unit employs more than 150 internal and around 20 external employees. Its IT department has a comprehensive set of l IT capabilities to support the variety of needs in the institution. This also includes a separate software development team that develops IT applications and tools for the institution's internal use by its staff and students.

The second institution has parts of its IT centralized, but a large part of its IT is decentralized within the various faculties. One of the decentralized capabilities in this institution is software development. The study takes place within the development team of one of those faculties. The team delivers software for employees and students of the faculty and even outside the faculty or institution. One of the developed applications by the team was actually also used and delivered to the first institution.

As both institutions process large amounts of privacy-related data (for example, names of students and employees, bank accounts, date of birth, et cetera), both institutions are subject to the GDPR, specifically articles 2 and 3 GDPR (EU, 2016).

3.4. Participants in the study

To answer the selected research questions, it is necessary to learn more about the opinions of developers who develop a variety of applications to users. In the first organisation the developers were asked to participate during a daily stand-up and three employees were randomly invited. At the second organisation the IT manager was approached and asked to find two developers and three users which met the criteria.

The selection of interviewees was based on the following selection criteria:

- Six users (three in each organisation) who use applications developed by the internal software development team;
- Four application developers (two in each organisation), with at least 10 years experience with software development.

The following table gives a summary of the respondents that were selected:

Respondent	Role	Position	Experience
University 1:			
UNI1DEV1	Developer	.Net developer	20 years as developer
UNI1DEV2	Developer	.Net developer	24 years as developer
UNI1EMP1	Application user	Liaison officer research	1 year employed by organisation
UNI1EMP2	Application user	Service and contract manager	10 years employed by organisation
UNI1EMP3	Application user	Location manager	7 years employed by organisation
University 2:			
UNI2DEV1	Developer	Application developer	14 years as developer
UNI2DEV2	Developer	Application developer	20 years as developer
UNI2EMP1	Application user	Associate Professor	19 years employed by organisation
UNI2EMP2	Application user	Analyst	5 years employed by organisation
UNI2EMP3	Application user	Lab technician and operator	18 years employed by organisation

Table 2: Participants for this study

3.4.1 Data collection

The unit of analysis for this research is the development process of application software.

To answer the question how users perceive privacy as a value, in-depth interviews with users have been conducted as a first step. Information or themes that have derived from this gave insight not only how they value their privacy, but also if users are aware of their privacy-related rights. To assess their knowledge about the threats that they are facing, Solove's model has been used (Solove, 2006). Users were also asked what they thought about PbD and the use of an approach such as the Value Sensitive Design method when developing software. After the user interviews, two developers were interviewed. The aim was to find out whether developers were aware of the legislation regarding to application and what PbD meant and how the organisation could operationalize this. In addition, the aim was to identify whether developers were familiar with the PbD principles (Cavoukian, 2009) and whether they actively used them. Furthermore, did users know the VSD approach and did they use it. If not, did they see added value in the approach? Were developers aware of the value of privacy their users have and how did they feel about PbD and the use of an approach such as VSD. The gathering of information has been performed in a cross-sectional way, whereby a snap-shot of the current state was made, which is in contrast to a longitudinal study where a phenomena is studied over an extensive period of time (Saunders, 2016).

The data collection phase comprised interviews that were performed in an open and semi-structured way and lasted a maximum of one hour. This enabled the researcher to continue asking questions, to elaborate on answers or to have them specified or quantified. All respondents were also asked for their permission to collect background information about the number of years in role, current and if applicable previous functions. Interviews were performed in Dutch and audio recorded; transcripts were also in Dutch. All interviews were transcribed with the consent of the interviewees, after coding in MaxQDA the transcripts were shared with the interviewees to give them an opportunity to react. Coding was also done in Dutch while quotes for the findings were translate into English. (The interview protocol can be found in Addendum A). To respect the interviewees privacy their names and case organisations will remain confidential.

3.4.2 Data analysis

The analysis of the collected data consisted of analysing the detailed verbatim transcripts made for every interview using an in-vivo coding approach as proposed by Strauss and Corbin (1990) and Saunders (2016). This involved apart from open coding that all selected sections were then axially combined into codes which were then being grouped based on theme. Finally, a round of selective coding followed (Gioia, Corley, & Hamilton, 2013). For the transcribing and coding process a specialised tool, MaxQDA, was used to create and maintain overview of the gathered data. This tool helped in building tree structures of the identified codes to help identifying themes which are presented in Chapter 4.

3.5. Reflection on validity, reliability and ethics

This section will focus on the validity, reliability and ethical aspects in relation to this study.

There are three types of validity to be distinguished: internal validity, external validity and construct validity (Saunders, 2016).

- *Internal validity* relates to the extent to which the results of the research allows for credible conclusions. In this study the researcher and supervisor ensured that internal validity was achieved in the design of the data collection protocols by both coding an interview and compare results.
- *External validity* is the extent to which the results can be generalized to units other than the unit of analysis (Saunders, 2016). Due to the exploratory nature of this research and the newness of the phenomena being investigated, the conclusion can be drawn that the findings will be too limited to extrapolate to a larger group.
- *Construct validity* is important for being able to draw conclusions from the research results. This means that the measurements must be performed correctly, so that the measured results are actually the results (Saunders, 2016). To guarantee this triangulation has been performed where multiple sources of data have been used through interviewing 10 respondents from 2 different organizations.

A few other examples (and corresponding measurements for this study) of problems relating to validity are:

- **Bias**: This considers the researcher's paradigm in which he conducted the research. In this study this was mitigated by conducting multiple interviews within two organizations. Privacy as bias was also to be expected, hence the findings in the literature that relate to the perception of privacy by individuals (Kokolakis, 2017). Furthermore, the researcher is working for one of the organizations since October 2019, and since he is not yet fully established in the culture of the organization, this bias was not considered a problem;
- **Socially constructed answers**: People tend to give answers which are socially acceptable (the so-called Hawthorn effect), especially considering sensitive subjects. This is something that the researcher kept in mind while processing the results. Measurements to minimalize these responds were a private setting where the interviews were held and anonymization of the results. In addition, similar questions were asked to multiple participants;
- **Non-response**: This was not a problem in the end as the study was welcomed by both units in both organizations.
- **Anonymity:** In this study no interviewee or organization names are recognizable through the use of acronyms.
- **Problems with interpretation of answers**: In this case with interviews, answers can be explained differently, or sometimes non-verbal communication can add a much to the spoken words. To mitigate this issue, the transcripts were offered to the interviewees giving them the possibility to add or change answers if the transcript does not reflect their intent regarding the answers.
- **Self-selection**: if people would voluntary participate in the research, there is a danger of self-selection where you might encounter a homogeneous group of respondents. To prevent, this the interviewees in this study were selected based on their role and function and were not known to the researcher?

3.5.1. Reliability

Reliability is about the possibility to repeat the research (by others) with the expectation that consistent results will be found (Saunders, 2016). For this research, reliability has been mitigated with the following measures:

- Extensive elaboration on the different methodology steps and type of data to be collected;

- Following sound reliable research principles and procedures;
- Periodically feedback from (V)AF mentor and assistance with analysing interviews (both researcher and supervisors coding, comparing and regularly discussing results);
- Sharing the transcript of each interview with each participant; and
- Conducting interviews with more than one role that are similar in nature so that the data collection could be triangulated, and
- Conducting the interviews within two separate organizations.

These measurements contribute to the reliability of the study.

3.5.2. Ethical aspects

After a series of misconducts by researchers, the Royal Dutch Academy for Science (KNAW) has created a memo regarding the ethical aspects and integrity for researchers in 2001. This evolved to a code of conduct for scientific integrity co-drafted by institutes and companies associated with scientific and academic education in 2018 (KNAW, 2018). The researcher considered himself bound by this code of conduct. A few other ethical aspects were considered:

- Assure anonymity for all interviewees;
- Respectfully saved their data (e.g. audio recordings and transcripts);
- Give interviewees the opportunity to withdraw themselves from the research.

4. FINDINGS

After an in-depth analysis of the data using the three-step qualitative coding technique (open, axial and selective coding (Corbin & Strauss, 1990)), the following themes arose. The data coding trees are available in Attachment B for every theme. Using the major themes identified in the literature review (Chapter 2), privacy-related themes of employees and developers are presented across both institutions in sections 4.1 and 4.2 that follow.

4.1. EMPLOYEE VIEWS

At both institutions, employees were first interviewed to ask them about their opinions, knowledge and views regarding privacy. Here follows an overview of the highlights that had been found within these interviews.

4.1.1. Employee views on the 'value' of privacy

All employees responded positively on the question how aware they were of their privacy. They see privacy as something that defines them and makes them a unique person, as one employee denoted:

> *You are an individual and for that you need privacy. It goes all the way to the core of the people (UNI1EMP2).*

Another employee added to this by saying:

> *[...] in my view, privacy is all that is actually more of me, which I consider important. Data [is] … what basically makes me, me (UNI1EMP3).*

But the responses also showed a privacy paradox whereby in exchange for a service, employees would give out their personal data. Despite this, employees where quite aware of their personal privacy as one employee said:

> *No, not so consciously [my awareness of privacy]. I would like to be more aware of that, or at least I may be partly aware of it, but I'm not acting on it (UNI1EMP3).*

All but one employee stated the selective attitude users have regarding their privacy. At moments they were very aware of their privacy, but they recognized how easily they gave their privacy away when using apps from Facebook and Google. An interesting confession of over half of the employees was that they prefer functionality of a tool above the privacy the tool has on offer:

> *But it is so nice to use* [WhatsApp] *that I take all those other* [privacy-related] *things for granted (UNI2EMP3).*

When asked why they acted in such a contradictory way, similar answers appeared. Employees recognized that functionality won the battle over their privacy when considering using an application, also the lack, or ignorance, on privacy friendly alternatives weighed in on the decision. Also, one confession related to social influence, if an alternative was at hand, but if no social contact uses it, then it is useless for social interaction. All but one interviewed employee said they were willing to pay for a privacy-compliant alternative by saying:

> *[...] but then I think about whether I would pay because it is safe or because I just need it (UNI1EMP3).*

Half of the employees mentioned another reason for their slack attitude towards privacy - they defined privacy as something you are unaware of - something which is intangible. They felt only once privacy is breached or violated you see negative side effects of disclosing your privacy. So as long as there are no consequences, it is hard to act on privacy:

So, if my identity were to be stolen sometime and it bothered me a lot, it would become a bit more tangible [...] (UNI1EMP3).

Furthermore, none of the employees could ever remember a moment that they have later regretted giving information in exchange for services. The remarks regarding privacy versus usability and the balance between both sparked another topic, *what about your privacy relating to security*? This gave a less clear picture. Two employees remarked that they were willing to surrender a little part of their privacy for the benefit of their security, if properly regulated. But there was also resistance to the idea that the government could use privacy- related information for security purposes:

[using information to increase] national security, so we can do anything. And I am against that, yes, then you will get Chinese conditions, and yes, everyone, I think everyone is very naive about that, in the Netherlands, because we are a safe country […] (UNI2EMP1).

Another employee confirmed that he would rather surrender his privacy for functional benefits than trading it for security. A third remarked that once data was gathered it is 'out there', so who knows what will happen in the future with data now collected due to government actions:

I think I am especially suspicious of the government, frankly. Not necessarily to this government. [...] but they have that information once. I don't know who will be in power for another ten years and what could be worse with it [privacy attitude of the government] or in 20 years (UNI1EMP1).

One remarkable finding during the interviews was "trust". Five out of six employees expressed more criticism towards developers from commercial applications they use in private than in-house developers of applications which they know and use at work. When asked upon why, they remarked they trusted the in-house developers of their own organisation more in handling their privacy correctly. One employee could not imagine that a large institution as theirs would not have a proper team that thoroughly thought of privacy matters:

I have great confidence in what is being developed here, I believe that it is more difficult to access things here than it is being made easy. I think we have a high priority here (UNI2EMP1).

Some more reactions based on trust by the employees were:

I also assume that if you build an application internally, it is really purely for the functionality and not for the financial gain and so that these principles are not only good for privacy, but also for an efficient and well-functioning app. I can imagine that (UNI1EMP1).

So, it's in good faith, in the end, I also know that they have some important information about me that they just need to be able to provide a service (UNI1EMP3).

[...] so I notice at least that enough is being done with privacy and that it gives me confidence [in the application] (UNI2EMP1).

4.1.2. Employee views on the GDPR

The second theme brought under the attention of the employees was the GDPR. All employees heard of the GDPR and remembered its introduction in May 2018 and knew that the GDPR relates to privacy. Only one employee mentioned that the GDPR brought him new rights regarding his information and privacy and could actively sum up a few of his rights brought by the GDPR. The responses of all other employees confirmed little substantive knowledge regarding new rights the GDPR brought to them, as one of them commented:

I mean in detail you will not have to ask me about the legislation and about it. So yes, everything that has to do with personal data, yes, that you have to be careful with that and I can also endorse that (UNI2EMP1).

Four out of six employees had an immediate association that the GDPR brings difficulties in their personal life, for example in their function as a volunteer for a soccer club:

[...] because the big companies ensure that they can work with it [GDPR] and I rather think that the small parties only suffer from it, such as a football club who only does membership administration and have to go to a lot of trouble [in doing so] (UNI2EMP1).

Upon further questioning, a few benefits of GDPR regulation became apparent: You have to be cautious with sharing data of others (two employees), you have to be precise what information you store (one employee), and you cannot take pictures and share them without permission (three employees):

[...] if, for example, you still want to publish photos and still need to have everyone's agreement [...] (UNI2EMP2).

4.1.3. Employee views on Privacy by Design

The third theme discussed was privacy by design, as the GDPR expect applications to comply to. As stated in Chapter 2 there is a clear connection with the 7 Privacy by Design principles (Cavoukian, 2009). These principles were introduced to employees and asked what they felt or thought about it. None of the employees knew anything about these principles in the form they were presented, but upon further discussion there were many positive remarks as two employees commented:

Everything you have given so far will contribute to increased privacy (UNI1EMP2), and

Yes, I never heard of them as seven principles, but it all makes sense that you should think about this when you ask people for data (UNI2EMP3).

Each principle could count on support from the employees, only a few annotations were to be made. The principle of "positive sum" sparked two remarks regarding the balance of what information you need for your application to function and what information you should not process regarding the user's privacy:

Yes, that is difficult, that is of course very much due to the application, isn't it? You do, for some applications you need to know more from people to ask or do what you want them to do (UNI2EMP3).

Although the seven principles where conceived as "stating the obvious", two remarks were made about the concreteness of the principles. Before developers can use these principles, they have to make clear exactly what they meant to incorporate in software development, maybe accompanied with examples:

If they [the principles] are tightened up a little [...] but maybe supplemented with some examples, or ... [I: made more concrete?]… Exactly (UNI2EMP2).

4.1.4. Employee views on software development

Employees were also asked about their views on the software development process and the privacy guaranteeing aspects giving by an application. Upon asked if they currently see *privacy-compliant guarantees in software applications* several comments were returned. One employee saw the inability to access other people's data, another one mentioned providing a personal login. Another guarantee one employee mentioned is the ability of applications to anonymize data. Also, one employee mentioned the importance of a privacy policy, although it was being described as (perhaps) intentionally long and difficult reads:

[...] so much fine print that no one goes through or very few people [do] (UNI2EMP3).

All employees were asked if they wanted to contribute to the software development process by delivering input for the development team regarding privacy. All confirmed they wanted to share their thoughts and opinions to a greater or lesser extent. Examples to do so were mentioned in the form of questionnaires, interviews or active participation in the software development process:

> *As a user, if I would eventually start using an application and then I have the choice to be able to think along, then I think I would indicate in what way [developers should protect my privacy] Then I would indicate to the development team that they must undertake as many actions as possible to ensure the privacy of me as a user (UNI1EMP3),* and

> *For example, through surveys or perhaps also talking to each other whether [privacy] is really necessary to have in it [the software application] (UNI2EMP2).*

At the end of the interview employees were confronted with a three stage approach for software development, the Value Sensitive Design method (Friedman et al., 2002). All employees recognized it as an easy to use process which would give them as users more confidence in the development of a new applications a place and voice in the process. They saw it as a logical construct as described by one of the employees:

> *I think this makes sense, you start thinking [about privacy] and [then] you test it [with the users], then you make it (UNI1EMP3).*

Employees were asked if in their opinion, the use of the VSD approach to develop software would benefit the privacy-compliance of applications. All employees responded positively, with one employee denoting that this approach would not only be beneficial for privacy aspects:

> *I think not only privacy friendly, but also user friendly. Just as a complete [structure], maybe It's a bit difficult to implement for application developers, or a bit more work (UNI2EMP2).*

4.2. DEVELOPER VIEWS

After interviewing employees, software developers where asked several questions regarding the incorporation of and focus on privacy principles in their software development processes. The following are the most remarkable themes that emerged.

4.2.1. Developer views on privacy

When asked about privacy, software developers' first response was that an application or tool should not gather too much data, especially unnecessary data that is not required for the proper functioning of an application. Two of the four developers indicated privacy was not important for them earlier:

> *[…] when I started 20 years ago, […] I actually didn't think about it [privacy] at all, I wanted to solve the problem and I was somewhere in the code and it would be useful if I had data from those [people], that is right there, you know, it works (UNI2DEV2)!*

As the second stated:

> *[...] because it always happened in the past, let's save everything, because that's handy. Suppose you need it later or whatever, then you already have it. Of course, we started to think a little different about that [...] (UNI1DEV2).*

Three out of four interviewed developers reacted positive on the GDPR, as they thought it offers more clarity about what is and is not allowed regarding privacy. One of those three and the fourth did mention that maybe GDPR is a bit too strict in relation to the handling of users' data:

> *I think it's good to pay attention to the data that applications store from users. On the other hand, I think we may exaggerate a little bit. (UNI1DEV2).*

Another reacted when asked about what they think of GDPR the following:

> *Very well of course. Yes, and I also think that everyone is seriously involved in this [GDPR compliance] and that it [GDPR] is maintained (UNI2DEV1).*

The developers all had over 10 years of experience with developing software applications. During their career they themselves developed novel forms and sorts of coding. When asked if any of their software development education and training ever focused on embedding privacy in the development process and final applications, they all responded negatively. IT training seems to have not been privacy-focussed within application development as one developer responded:

> *What you see in IT, in an IT course itself, is actually very technology driven (UNI1DEV2).*

4.2.2. Developer views on Privacy by Design

Also, with developers there was a discussion regarding PbD. Although developers heard about the term mostly in relation to the GDPR, none of them ever heard about the 7 PbD principles as constructed by Ann Cavoukian (2009). The discussion of these seven principles sparked enthusiasm with the developers. They could directly relate the principles to their work and how they handled privacy, but they also saw many additional and useful guidelines that could be incorporated and used in their work as two software developers commented:

> *Yes, that [principle] is something that I advocate with a lot of things. I like to think first about how things should be done (UNI2DEV2)*, and

> *[The principles] Sounds logical. I cannot disagree with any of them. I have to admit that anyway (UNI1DEV1).*

Although there was a positive attitude towards the 7 PbD principles, a few remarks were made. One remark was that *it must be workable (UNI1DEV1)* to perform, because it would take significantly more effort to embed al these principles within the design and development process. Although they thought that some principles could be a more precise or concrete, one should watch out to exaggerate:

> *[…]it [the principles] should not be, should not become a study, before you can meet them [the principles] (UNI1DEV2).*

All developers confirmed that the privacy aspects of an application would benefit from using and adopting the privacy by design principles within their software development process. They all indicated they wished to receive a copy of the 7 PbD principles after the interview to gain more knowledge about them and potentially incorporate and use the principles within their software development process.

> *Yes, I think it is very good that we will address this [the principles], as developers to go through them (UNI2DEV1).*

4.2.3. Developer views on the VSD approach to software development

Developers were also presented with the Value Sensitive Design (VSD) method (Friedman et al., 2002). They were asked several questions relating to using this method for embedding privacy within the software development process. They acknowledged that the proposed staged method would give employees a place within the process and offer them room for addressing their concerns. Ultimately, they unanimously agreed that using a method would result in more privacy-compliant applications:

> *[...I] think that this [VSD method] is a structured way that we can benefit from. (UNI2DEV1).*

And that the method forced a software developer to interact with their users:

The advantage of structured working is that they [users] are of course involved from the start and you see [points at model], in the beginning everything is considered exactly what they [users] want (UNI1DEV2).

Two developers mentioned that it would take extra time and effort to follow the three stages of the Value Sensitive Design method, mostly because of the feedback loop where you would have to go back and forth to your stakeholders:

Those [feedback loops] are all, time consuming things, I think (UNI2DEV2).

One developer indicated that one could only find out if the downsides of using this method outweigh the benefits of the software development process by trying it out:

Look if you say after ten times: Yes, we have followed it [the VSD method] ten times and nothing ever comes out of it, then you can also conclude: Apparently, maybe it is not necessary. Or you say you just keep doing it (UNI1DEV1).

One developer remarked that using a form of a checklist within the stages of a structured software development method would be useful to have a discussion regarding privacy with the users serves as:

[…] a structured list of things to go through are a very good handle for this [privacy matters] (UNI1DEV2).

When asked the question, all the developers unanimous agreed to the fact that using a method would benefit the privacy-compliance of an application

4.2.4. Developer views on the employee perceptions

During the interviews, developers were asked regarding some topics what they think what the employees would think or say about the items which we were discussing. This last theme gives insight on how developers view their (end)users.

When talking about users and how software developers would interact with them during a software development process, the developers all actually alluded to the interaction with their 'client'. The client is the owner or instructing party to develop software. In this context, the software developer does not see the clients as a separate entity from the end-users (those who actually use the software during their day job). The client in this context most often was the person who gives requirements to developers instead of the end users who are intended to use the software. Users were therefore represented by the 'clients'. Software developers had no insight if the clients would talk to the (end)users. One developer said:

If they [the client] discuss anything with their customers [users] at all, I [the developer] don't know. I have no insight into that (UNI1DEV1).

In this context, none of the developers actually involved their end-users directly in the software development process, or even asks them about privacy-specific aspects:

So actually, now that you are talking about it [involving end users] it [their wishes] is not directly discussed with the customer 1 on 1 (UNI1DEV2).

At one of the participating institutions it was in some cases common practice to consult administrators or key-users to gather requirements, which was only a small and specific group of end-users. But developers of this institution also said that this does not cover end-users as a whole. Put in context, it was clear that this approach could be a surprise for end-users, for example in this case end-users would be students, as one developer indicated:

[...] that is unfortunately not [done] here [involving end users], what I say [is] the students are often, the indirect object and they often only see that there is a new system

[that they need to use] […]. Then there is sometimes complains or groans, but yes that is actually quite late (UNI2DEV2).

As noted earlier, all developers acknowledged the importance of privacy and embedding privacy as a value in their applications. Despite this, they also conceived users of their applications often not to be as *privacy minded* as they say they were. These seemed ambiguous behaviours from users, and a direct effect of the privacy paradox:

[….] people [end-users] shout very loudly: 'Oh, my privacy is a thing', but then [they] put on Facebook everything they want to put down, it is open and it is shared (UNI1DEV2).

Or as another developer summarized it:

[...] you can organize it all perfectly technically, they remain people, users are people and they handle it more carelessly than you technically allow them (UNI2DEV2).

When the PbD principles were discussed, the developers would be asked how users would perceive the principles. While two developers pointed out that principle seven of PbD (Respect for the user's privacy) was the one that users would find important, another would say they appreciate principle 5 the most (end-to-end privacy protection). Three of the developers pointed out that most users would not care so much about the principles:

Most of it [the principles] won't say them [the users] much. Except the last [7th principle: respect for users' privacy] because most of it is mainly technical (UNI1DEV1).

When discussing the use of the Value Sensitive Design method for designing applications, the developers were asked how their users would perceive such an approach and applications that were developed using such an approach. Three developers stated that using this process would be perceived positively by users. Users would be more involved with the development process. The method adds more trust to the process and gives it a positive appearance. Finally, the users would have more insight into the approach and increase the existing trust that is already there:

Of course, there is [at this moment] trust, but it [adapting the principles] also makes it more transparent yes (UNI2DEV1)

One developer projected the user's interest on his own interest of other processes like within HR. He concluded that users would be more interested in the result than the process leading to the result:

[...] they just assume that it [the process] is just well organized, how you do it [create applications], not I think (UNI2DEV2).

During the interviews, trust was also discussed several times with the developers. Three developers acknowledged that a there was a large part of trust between them and their users on safekeeping their user's data. The importance of not violating this trust was also mentioned by one:

[...] you have to gain or lose trust, as it were. You can only lose it in general (UNI1DEV2).

5. DISCUSSION, LIMITATIONS AND RECOMMENDATIONS

This chapter give answers to the formulated main and sub research questions through a discussion presenting outcomes of this study. Furthermore, it highlights the limitations of this study and how the findings could be put into use for academics and in practice.

5.1. Discussion

To answer the main research questions (the sub research questions (SQ) will first be discussed and answered followed by the major research question.

1) SQ1: *What are users views on the value of individual privacy in context of the software development process?*

The answer to this question has multiple aspect, as summed up and discussed below:

- Employees 'entrusted' their data to processors with minor objections regarding their individual privacy, which is contrary to the statements they make that they feel their individual privacy is important.

All employees were aware of the value of privacy and recognised threats on their personal data, as Bashir et al (2015) also confirmed in his study. Contrary to Bashir's study none of the interviewees noted that they had ever regretted submitting personal information, where Bashir noted an 82% positive response. The employees were honest regarding the privacy paradox (Brown, 2001), i.e. on the one hand saying privacy is important for them, but on the other hand giving it away on other mediums. This behaviour is also something that developers see and address. While developers can attempt to build privacy-compliant applications, users continue to give away their information so easily through the use of modern social media applications such as Facebook and TikTok. This may be a result of users' ignorance or non-education in terms of the real data (personal data) being collected by different platforms and application by foreign entities. For example, the TikTok application that is now Chinese-owned by ByteDance is currently one of the most popular platforms used by over one billion (mostly) young generation people in the world (Pham, 2019). However, the collection of data (in the form of images and videos) by this application is controversial. There are many investigations about privacy concerns relating to the collection and use of children's data. For example, privacy authorities in the UK (Hern, 2019) and in the US have already settled millions of dollars related to this issue (Bergman, Frenkel, & Zong, 2020). A surprising finding was the balance between privacy versus functionality and privacy versus national security. Employees stated that they would easily trade their privacy in return for good functionality but were not as eager to trade their privacy in return for national security. The reactions were not so clear as what was to expect according Kokolakis' study (2017).

- Employee views indicate great uncertainty about the use of their data and lack of knowledge what applications (and processor) do with their data.

Users should be more aware about potential threats concerning their data. Understanding a model like Solove's (2006) will definitely help. The problem is that users mostly are short sighted. They only focus on information collection from processors and they have no idea what happens with information processing and dissemination. For example Zoom collects user's data (were users are aware of), but sends users data directly to Facebook, even if users do not have a Facebook account (Cox, 2020). Privacy policies should address these issues, what rights users have and indicate how users' data is being protected once collected and processed. For example in the case of TikTok the privacy policy '*basically states you have some rights'* (McGue, 2020). If users where more aware

regarding the scale of their data being (mis)used, they might be more positive towards the GDPR (which provides legislation from a user standpoint).

- Employees do not feel they are involved in the development process of an application.

A surprising finding of employees in both case organisations indicated that they were not actively involved in the software development process. Modern software development teams are often working with an Agile method that actively incorporate users in the software design process. Although the Agile Manifesto (Beck et al., 2001) values customer collaboration, the collaboration itself in this context was not with the end-user per se, but instead with the client who pays for the development of the application. Furthermore, user collaboration is not only needed and important in design or development, but also during the whole lifecycle of an application (Davis, 2020).

- Employees have great trust in the developers handling their privacy.

Trusting internal software developers was a surprising finding that was identified in the data analysis. Users in this context trusted the institution's internal software developers to handle their privacy properly, without really substantiating what that trust was based on. Developers also acknowledged this trust when asked about this aspect after an analysis of users' interviews. This relates closely to the field of Employee-Organization Relationship (EOR), where research indicates that if employers invest in their employees, a result is trust among co-workers, for example the research by Tsui et al (1997). Possibly, this is a factor why end-users have trust in their co-workers who create application(s).

2) SQ2 *How can applications become more GDPR compliant from using principles of Privacy by Design in the software development process?*

The answer on this question is that adaptation to PbD principles will help applications to become more privacy-compliant and contribute to more GDPR compliant applications. The 7 PbD principles offers a structured list that software developers can use to check their applications.

The discussion of the 7 PbD principles (Cavoukian, 2009) sparked a lot of enthusiasm with both employees and software developers in both organisations. The latter could relate many PbD principles with how they are handling situations right now or how they could improve their software development process. The employees were also positive regarding the principles and thought that software applications would benefit from adapting the existing principles within the software development process. It was mentioned that the principles in current form are somewhat abstract, so the principles could benefit from clarification and specification. A first step to do so is adapting the practical advice as Spiekerman and Cranor (2008) have set up in their research as can be found in Chapter 2.2.5 of this research.

The developers thought that most of their users would only appreciate one or two principles from PbD, but in discussion with employees, they only remarked two minor objections with the principle of 'full functionality'[2]. The other principles where received with great enthusiasm and shows that end users are more invested than software developers attribute them. This presents that developers could and should do more with the views that users have on system design and development to improve applications, as previous research also indicated (Procaccino & Verner, 2009).

This research made an effort to determine if adoption of the PbD principles will contribute to privacy-compliance of an application and therefore ensure for more GDPR compliant applications. Both interviewed groups confirm that in their opinion the privacy-compliance of applications would

[2] Full Functionality: *"Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both."* (Cavoukian, 2009).

be increased by adopting to PbD principles, this was also concluded after the literature review. Although it does not give a 100% guarantee success, based on the literature review and information that for example the ICO gives (ICO, 2020), one could conclude that adapting the 7 PbD principles could result into GDPR compliant applications.

3) SQ3: *How can applications become more GDPR compliant from using principles of Value Sensitive Design?*

Having identified in previous SQ's the value of ones' privacy and the usefulness of PbD principles, the remaining question is how to embed these into the software development process. The general answer on this question is two-fold:

- Both employees and developers agree that adopting a method like VSD, would extend the privacy-compliance of an application. By combining this with the values of users and with the PbD principles, it is more likely that it will result in more GDPR-compliant applications.

When presented with the VSD method (Friedman et al., 2002) both employees and developers in both organisations reacted positively. They saw it as an improvement to involve users and to think about privacy in the early stages of the software development process, as confirmed in previous research by Ligtvoet et al (2015). So, both software developers and employees agree that adapting VSD would contribute to the privacy-compliance of applications.

A possible negative side effect found in this research was the extra time it would take to follow the method. Furthermore, the shift in paradigm from creating requirement-based applications to value based applications is also a significant step developers need to take. One could ask if developers see the necessity and have enough autonomy to shift to this new way of working (Bednar, Spiekermann, & Langheinrich, 2019), even if they see the value in the proposed method as this research found. Implementing VSD into applications can be challenging and to find the right path, developers can look for support into the 14 design methods reviewed and proposed by Friedman et al (2017).

- Software development methods currently have little focus on the individual privacy of their users and can improve to create more GDPR-compliant applications.

From a privacy perspective we see from the literature that there is movement to enlarge privacy-compliance of applications, like creating a privacy impact assessment within an Agile way of working (Clearwater, Quayle, & Ort, 2016). This is in contrast to influential Agile methods for example SCRUM, that does not even mention the term 'privacy' (Sutherland & Schwaber, 2017). This ties closely to a relevant finding, which was that the performed literature analysis in this research did not come up with any results on privacy within software development education, only one article mentioned the lack of education on privacy for developers (Cummings, 2006). All developers pointed out that in their careers (with an average of almost 20 years) they never saw privacy as part of their education or training. This could be attributed to the relatively recent focus on big data and privacy as a technical issue in software development. It is somewhere disappointing that popular software development methods based on Agile principles, e.g. SCRUM or SAFe, do not mention privacy or even privacy values of users (Beck et al., 2001; SAFe, 2020; Sutherland & Schwaber, 2017). In relation to current focus on privacy there lies an opportunity for methods to embed privacy.

MQ: *How can Value Sensitive Design and 'Privacy by Design' embed Privacy Values into software development to develop applications that are more GDPR compliant?*

The prior answers lead to a response on the final MQ. The research confirmed that the Value Sensitive Design method can combine the value of privacy from end-users and PbD principles to create

applications that are more privacy-compliant, which in turn contributes to more GDPR compliant applications. This confirms the conceptual model as presented in Chapter 2 of this research. So, organisations should think on how they incorporate the principles of PbD and VSD as part of their software development process to implement privacy values of their users. Examples to achieve this can be 1) involve users in an early stage, 2) create checklist(s) for developers to use during development or 3) embed these checklists also within test procedures of software applications.

5.2. LIMITATIONS

This research has some limitations, as summed up below:

I. First, the case organisations did not display many differences in results, so comparison between the two organisations was marginal possible;
II. The second is the use of case-study research in this context, although performed in two separate organisations to enlarge generalizability, is limited (Saunders, 2016). The study took place in two universities, but there are many universities and besides that government organisations, private companies et cetera, which could have different findings. The earlier mentioned limitation on differences between the organisations were positive in this context as it strengthened the findings. Furthermore, the founded trust in the handling of data by co-workers has influence on generalizability, it is likely that people feel different in organisations where they are less valued by their organisation. To confirm the applicability of the founded results in other organisations, research should be extended to a general population (with no affiliation with the development team) and other organisations;
III. The third limitation is the number of respondents using interviews with a small sample size (n=10). In future research other means of collecting data can be useful to triangulate the themes as found in this research.

5.3. RECOMMENDATIONS FOR ACADEMICS AND PRACTICE

The research gathered a lot of insights and rich data which can be used by academics and in practice.

5.3.1. Recommendations for academics

Future research could continue researching this subject and continue on the following items:

I. Future research could quantify the effort to shift to value-based software development and to what extent this effort outweighs existing benefits. This research could also focus on specific conditions engineers need to make the shift to creating value-based applications;
II. The literature analysis in the research made an effort to look at the GDPR from design-perspective and provide evidence that requirements from the GDPR on PbD were covered by Cavoukian's principles (2009). Future research with a bigger emphasis on a legal point of view could confirm if adopting these principles do in fact lead to applications that are more GDPR compliant. This research could also focus on developing a checklist using the principles of PbD and VSD.
III. Future research should give more insight on the balance between privacy and functionality and the balance between privacy and (national) security. When do users trade off their privacy for functionality or for (national) security?;
IV. Future research could further explore the addition of PbD as a subject within software development education and its impact on the development of privacy compliant software applications.
V. The field of Employee Organisation Relationships could contribute to explain how privacy as a value is perceived in an organization based on trust (in the organisation and/or co-workers).

5.3.2. Recommendations for practice

The findings of this research can already lead to a few improvements that managers or teams could put into practice:

I. Discuss Privacy by Design principles within your software development team and encourage them to use this as a checklist at the start of new application development. This will ensure that no privacy aspects are overlooked and that more privacy-compliant and hence more GDPR compliant applications are developed;
II. Identify if incorporating principles of the VSD method can ensure that end-users are involved in the conception phase of new applications. This will ensure that end users have a more prominent place in the beginning of and throughout the software development process and that their values on privacy are picked up during an early stage of this process. A structured approach will also mean a grounded and well-founded approach which will lead to more privacy-compliant applications.

REFERENCES

ABDC. (2019). Current ABDC Journal Quality List. Retrieved from https://abdc.edu.au/research/abdc-journal-list/

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). *Online privacy and informed consent: The dilemma of information asymmetry.* Paper presented at the Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community.

Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., . . . Jeffries, R. (2001). The agile manifesto. In: Feb.

Bednar, K., Spiekermann, S., & Langheinrich, M. (2019). Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society, 35*(3), 122-142. doi:10.1080/01972243.2019.1583296

Bergman, R., Frenkel, S., & Zong, R. (Producer). (2020). Major TikTok Security Flaws Found. Retrieved from https://www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html

Braster, J. F. (2000). *De kern van casestudy's*: Uitgeverij Van Gorcum.

Brown, B. (2001). Studying the Internet experience. *HP LABORATORIES TECHNICAL REPORT HPL, 49*.

Burmeister, O. K., & Kreps, D. (2018). Power influences upon technology design for age-related cognitive decline using the VSD framework. *Ethics and Information Technology*, 1-4.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada, 5*.

Cellan-Jones, R. (Producer). (2019). British Airways faces record £183m fine for data breach. Retrieved from https://www.bbc.com/news/business-48905907

Clearwater, A., Quayle, C., & Ort, C. V. (Producer). (2016). An Agile Approach to PIAs and Privacy by Design. Retrieved from https://iapp.org/media/presentations/PSR_2016/PSR_2016/An_Agile_Approach_to_PIAs_and_Privacy_by_Design_PPT.pdf

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology, 13*(1), 3-21.

Cox, J. (Producer). (2020). Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account. Retrieved from https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account

Cummings, M. L. (2006). Integrating ethics in design through the value-sensitive design approach. *Science and Engineering Ethics, 12*(4), 701-715. doi:10.1007/s11948-006-0065-0

Davis, A. (Producer). (2020). What's Next in DevOps? . Retrieved from https://www.infoq.com/articles/what-is-next-devops/

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14*(4), 532-550.

Espiner, T. (Producer). (2018). GDPR: 'Don't panic!' data watchdog tells firms. Retrieved from https://www.bbc.com/news/business-44208456

EU. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Friedman, B. (1997). *Human values and the design of computer technology*: Cambridge University Press.

Friedman, B., Hendry, D. G., & Borning, A. (2017). A survey of value sensitive design methods. *Foundations and Trends® in Human–Computer Interaction, 11*(2), 63-125.

Friedman, B., Kahn, P., & Borning, A. (2002). Value sensitive design: Theory and methods. *University of Washington technical report*(02–12).

Friedman, B., Kahn, P. H., & Borning, A. (2008). *Value sensitive design and information systems*.

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems (TOIS), 14*(3), 330-347. doi:10.1145/230538.230561
Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods, 16*(1), 15-31.
Google. (2019). Google Scholar Metrics. Retrieved from https://scholar.google.com/citations?view_op=top_venues&hl=en
Hern, A. (Producer). (2019). TikTok under investigation over child data use Retrieved from https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use
ICO (Producer). (2020). Data protection by design and default Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/
ISO/IEC/IEEE. (2017). Systems and software engineering - Software life cycle processes. In (Vol. 12207).
KNAW. (2018). Wetenschappelijke integriteit Retrieved from https://www.knaw.nl/nl/thematisch/ethiek/wetenschappelijke-integriteit
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. doi:10.1016/j.cose.2015.07.002
Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law, Computers & Technology, 28*(2), 159-171.
Leijten, J. (2019). Siri blijkt een slimme afluistervink. *NRC Handelsblad*. Retrieved from https://www.nrc.nl/nieuws/2019/08/08/siri-blijkt-een-slimme-afluistervink-a3969536
Ligtvoet, A., van de Kaa, G., Fens, T., van Beers, C., Herder, P., & van den Hoven, J. (2015). *Value Sensitive Design of Complex Product Systems*.
Lofland, J., & Lofland, L. H. (1984). A guide to qualitative observation and analysis. *Belmont, Calif.: Wadsworth. LoflandAnalyzing Social Settings: A Guide to Qualitative Observation and Analysis1971*.
McGue, T. (Producer). (2020). Is TikTok Raiding Your Privacy In 2020? Here Is How To Stop It. Retrieved from https://www.forbes.com/sites/tjmccue/2020/02/13/is-tiktok-raiding-your-privacy-in-2020-here-is-how-to-stop-it/
Oxford, U. o. (Ed.) (2020) Oxford Learners Dictionary. Oxford University Press.
Pham, S. (Producer). (2019). The company that owns TikTok now has one billion users and many are outside China. Retrieved from https://edition.cnn.com/2019/06/20/tech/tiktok-bytedance-users/index.html
Ponemon. (2019). *Keeping Pace in the GDPR Race*. Retrieved from https://mcdermott-will-emery-2793.docs.contently.com/v/keeping-pace-in-the-gdpr-race-a-global-view-of-gdpr-progress-in-the-united-states-europe-china-and-japan
Procaccino, J. D., & Verner, J. M. (2009). Software developers' views of end-users and project success. *Communications of the ACM, 52*(5), 113-116.
Provost, F., & Fawcett, T. (2013). *Data Science for Business: What you need to know about data mining and data-analytic thinking*: " O'Reilly Media, Inc.".
SAFe. (2020). Principle #10 – Organize around value. Retrieved from https://www.scaledagileframework.com/organize-around-value/
Santanen, E. (2019). The value of protecting privacy. *Business Horizons, 62*(1), 5-14.
Saunders, M. (2016). *Research Methods for Business Students* (7 ed.). Harlow: Pearson Education Limited.
Solove, D. J. (2002). Conceptualizing privacy. *Calif. L. Rev., 90*, 1087.
Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477-564. doi:10.2307/40041279
Spiekermann, S., & Cranor, L. F. (2008). Engineering privacy. *IEEE Transactions on software engineering, 35*(1), 67-82.

Sutherland, J., & Schwaber, K. (Producer). (2017). The Scrum Guide. Retrieved from https://scrumguides.org/scrum-guide.html

Tsui, A. S., Pearce, J. L., Porter, L. W., & Tripoli, A. M. (1997). Alternative approaches to the employee-organization relationship: does investment in employees pay off? *Academy of Management journal, 40*(5), 1089-1121.

UN. (1948). Universal Declaration of Human Rights. In U. Nations (Ed.).

van de Kaa, G., Rezaei, J., Taebi, B., van de Poel, I., & Kizhakenath, A. (2019). How to Weigh Values in Value Sensitive Design: A Best Worst Method Approach for the Case of Smart Metering. *Science and Engineering Ethics*, 1-20.

Warnier, M., Dechesne, F., & Brazier, F. (2015). Design for the Value of Privacy. *Handbook of ethics, values, and technological design: Sources, theory, values and application domains*, 431-445.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harv. L. Rev., 4*, 193.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Westin, A. F. (1967). Privacy and freedom Atheneum. *New York, 7*, 431-453.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European journal of information systems, 22*(1), 45-55.

Yin, R. K. (2014). *Case study research: design and methods* (Fifth Edition ed.). Thousand Oaks: Sage Publications Inc.

ATTACHMENT A: INTERVIEW QUESTIONS

In this attachment the used interview questions are placed which were used for the interviews during the data collection phase.

INTERVIEW QUESTIONS FOR DEVELOPERS

Do you know about privacy?
What do you think about privacy/GDPR
How does privacy relate to the GDPR?
Do you think privacy can be embedded in the software design process?
How was Privacy a part of your training/development to become a developer?
Do you know about Solove's model and the threats he has identified?
What threats are relevant for you as a developer?
Which threats do you think users think of as important?
How do you know what the users of your applications expect from privacy?
How do you think users appreciate their privacy?
Are users more or less aware regarding privacy due to the recent GDPR changes?
How do you currently implement privacy features in your development process?
How do you currently involve users in the development process?
Should privacy be hardcoded in applications?
What could be improvements of privacy within the SD process?
Are you familiar with the 7 Privacy by Design principles?
Do you think these principles are important?
Do you use these principles when developing an application?
How do you think that using these principles can improve the privacy aspects of an application?
What do you think that users find of these principles?
Which principles do you think are most relevant for your users?
What moments do you think users find important to give privacy related input into a development process?
What do you think of a SD process that also focusses on privacy?
What do you think of the importance of privacy as a value in the SD process?
How do you think about a structured method to embed privacy value(s) and privacy by design in an application?
How do you think such a method will improve the GDPR compliance of an application?
Do you think that such a method will improve the opportunity a user has to provide privacy related input into the software development process?
How will users think of an application that is developed with such a process?

INTERVIEW QUESTIONS FOR USERS

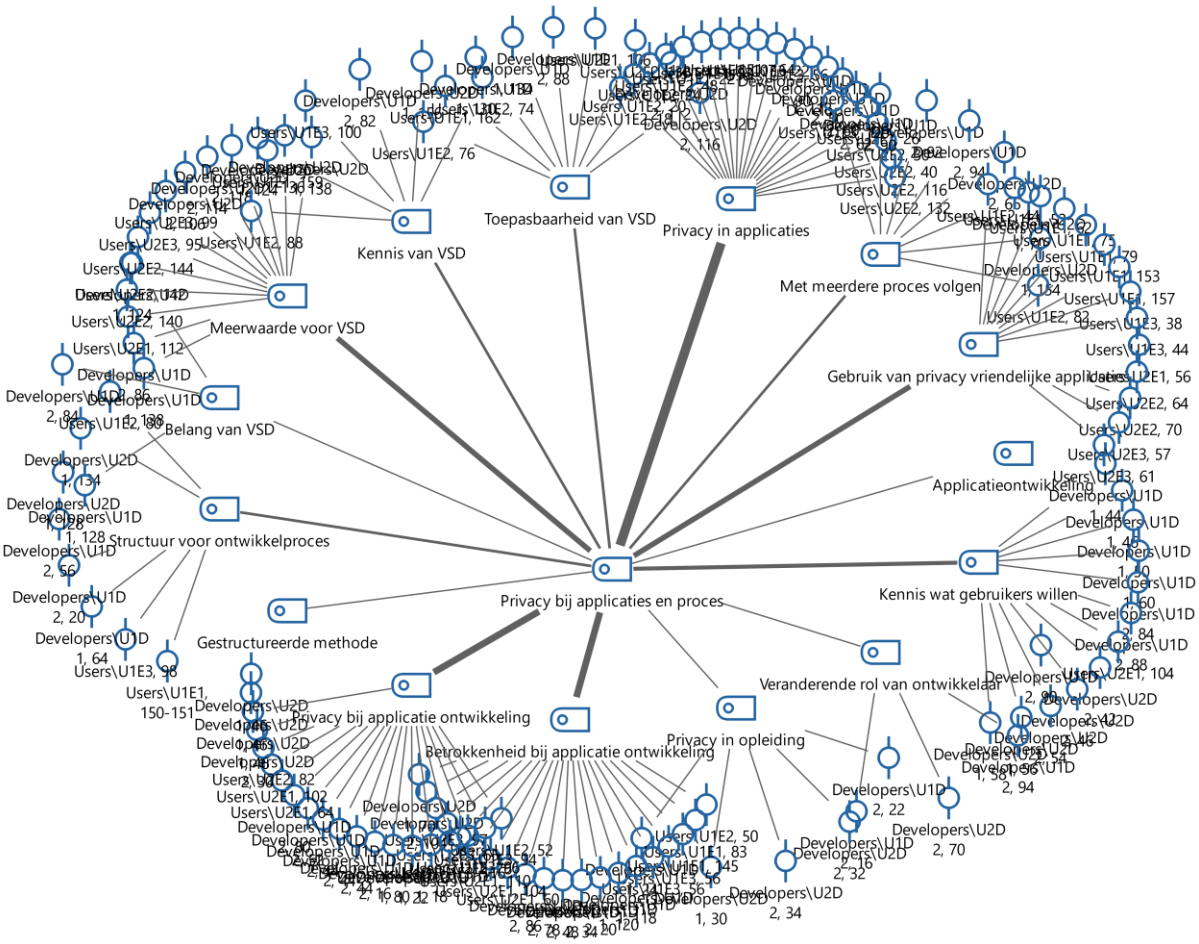
Ask about apps
Do you know about privacy?
What do you think about privacy/GDPR
How does privacy relate to the GDPR?
How important is privacy as a value for you?
Why is privacy (not) important for you?
What value of privacy do you recognize in current applications?

How should applications consider privacy values of their users?
Are you more or less aware regarding privacy since the GDPR introduction? > Why?
Do you know about Solove's model and the threats he has identified?
What threats apply to you?
Do you consider these threats when using an application? Why?
Have you ever decided to NOT use an application due privacy issues?
Did you ever had any regret sharing privacy sensitive information?
Are you more likely to use a privacy friendly application?
Would you pay for a privacy friendly application? Why?
How would you like to be involved in the development of an application by a development team?
Which privacy-related input would you like to give to a development team for a new application
What do you know about the 7 Privacy by Design principles?
What do you think of each principle?
Should developers consider these 7 principles?
What can developers do more to create privacy friendly applications?
What do you think of an application that has been developed in a structured manner where you can give input regarding your privacy concerns?
Would you be more inclined to use an application that has been developed with such a structured approach? > Why?

ATTACHMENT B – CODE TREES

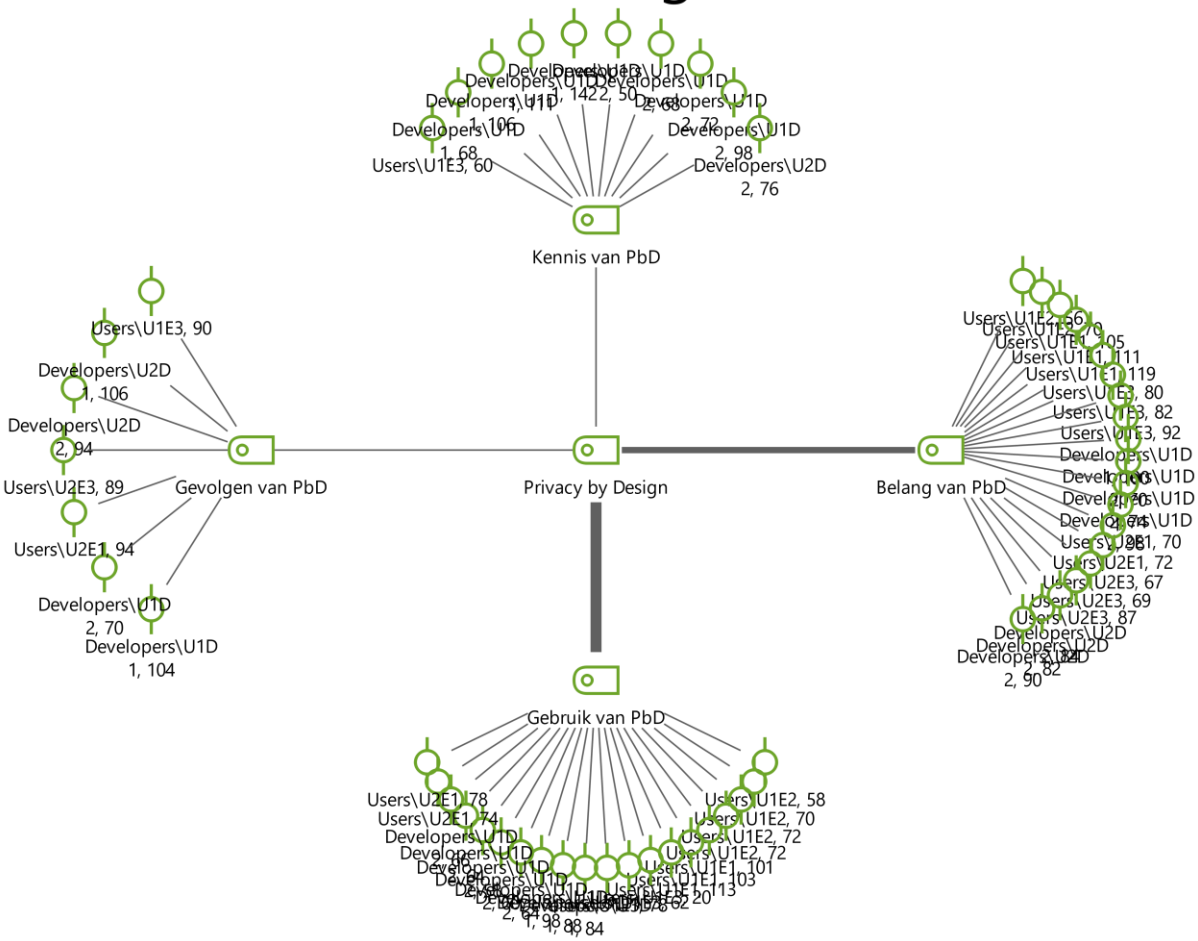
In this attachment four code trees are placed generated with MAXMaps in the MaxQDA software.

TREE 1 PRIVACY IN APPLICATIONS AND PROCESS



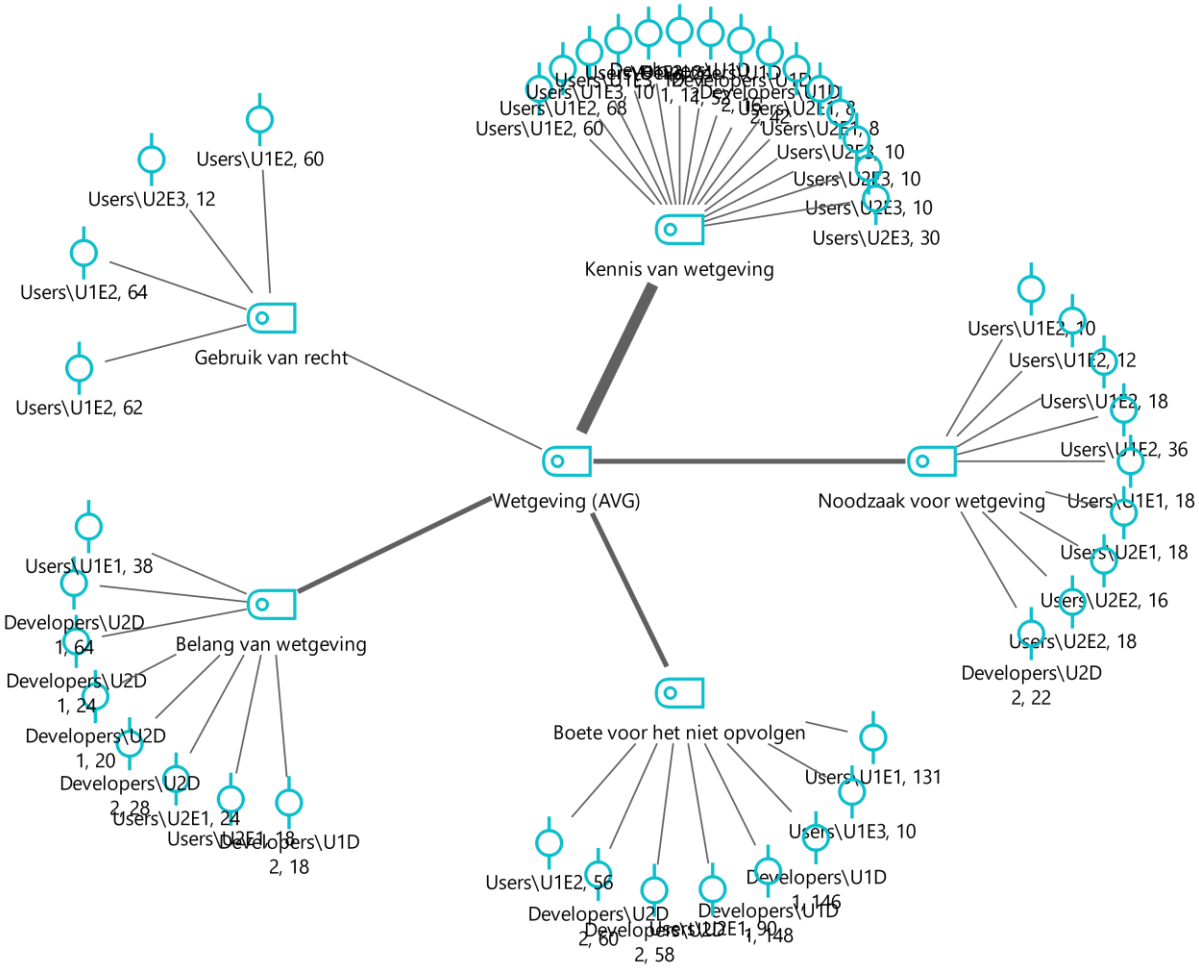
TREE 2 PRIVACY BY DESIGN

Code-Subcodes-Segments Model



TREE 3 GDPR REGULATION

Code-Subcodes-Segments Model



TREE 4 VALUE OF PRIVACY

Code-Subcodes-Segments Model